

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 17.06.00.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 21.12.01 Bulletin 01/51.

56 Liste des documents cités dans le rapport de
recherche préliminaire : *Ce dernier n'a pas été
établi à la date de publication de la demande.*

60 Références à d'autres documents nationaux
apparentés :

71 Demandeur(s) : *ESPACE.CX.COM Société à respon-
sabilité limitée* — FR.

72 Inventeur(s) : ALMES CHRISTIAN, TRIBY XAVIER
et FONT PHILIPPE.

73 Titulaire(s) :

74 Mandataire(s) : ROMAN MICHEL.

54 SYSTÈME DE SECURITE DE TRAITEMENT, DE STOCKAGE, D'ACCES ET DE TRANSFERT DE DONNEES
CONFIDENTIELLES.

57 Le système de traitement de données confidentielles
comprend au moins :

un premier ensemble de traitement des données com-
prenant au moins un serveur auquel sont connectés au
moins une première base de données, au moins un module
de saisie et d'enregistrement desdites données dans ladite
première base, après cryptage, à l'aide d'une première clé
publique corrélée à une première clé privée, enregistrées
dans une mémoire du serveur, ledit premier ensemble com-
portant au moins un module de lecture des données enre-
gistrées pourvu d'un lecteur d'un support avec mémoire
contenant au moins une clé utilisateur, corrélée au couple
première clé publique et privée, cette clé utilisateur étant uti-
lisable pour le décryptage de tout ou partie des données
cryptées,

un second ensemble de traitement et de stockage des
données, comprenant au moins premier serveur auquel
sont connectés au moins une première base de données
dans laquelle sont archivées les données confidentielles
préalablement enregistrées dans la première base de don-
nées du premier ensemble de traitement, ledit second en-
semble de traitement étant connectable au premier par des
lignes téléphoniques et/ ou spécialisées, et étant pourvu

d'un serveur constituant domaine racine, et générant un
certificat d'authentification racine comprenant deux clés ra-
cines publique et privée, ledit domaine racine étant apte
pour chaque premier ensemble à générer au moins un cer-
tificat d'authentification secondaire composé de ladite pre-
mière clé publique et de ladite première clé privée et pouvant
recevoir notamment du premier ensemble des demandes
de transfert de copie des données archivées, lesquelles
sont transférées après cryptage avec la première clé publi-
que.



SYSTEME SECURISE DE TRAITEMENT, DE STOCKAGE, D'ACCES ET DE TRANSFERT DE DONNEES CONFIDENTIELLES.

La présente invention est relative à un système sécurisé de traitement, de stockage, d'accès et de transfert de données numériques confidentielles par exemple de données
5 médicales relatives à l'état de santé de patients, clients d'un ou plusieurs centres de soins tels que cliniques, hôpitaux, et autres, ainsi qu'aux résultats des examens médicaux qu'ils ont été amenés à subir dans lesdits centres de soins, les résultats de ces examens médicaux étant matérialisés par des comptes-rendus écrits associés éventuellement à un ou plusieurs enregistrements d'images fixes par exemple des radiographies, et/ou à des images dynamiques,
10 par exemple des séquences vidéos d'échographie, et/ou des séquences sonores par exemple des séquences Doppler.

Les comptes-rendus écrits sont établis par le médecin en charge de l'examen médical.

Pour un patient, client de plusieurs services médicaux d'un même centre de soins, il est utile de pouvoir compléter d'un service à l'autre le dossier médical de ce patient sans devoir au
15 niveau de chaque service ressaisir les données de base telles que l'état civil du patient, par exemple son sexe, ses noms, prénoms, âge, profession, son numéro de sécurité sociale, sa caisse d'affiliation, sa mutuelle ou son assurance médicale. Les renseignements communs peuvent concerner aussi des données morphologiques telles que la taille et le poids, ainsi que les antécédents médicaux et les facteurs héréditaires. De même, peuvent être saisies des
20 données relatives aux degrés de dépendances du patient vis-à-vis de certains produits tels que le tabac, l'alcool etc.

Il est intéressant d'associer à ces données de base, d'autres données relatives à l'historique médical du patient dans le centre de soin. Cet historique pourra ainsi faire état des différentes pathologies tant médicales que chirurgicales, des traitements prescrits et de leurs
25 états secondaires.

Il y a lieu de noter que les différentes pathologies, les réponses thérapeutiques et les états secondaires associés sont codés pour une meilleure traçabilité des actes médicaux et chirurgicaux accomplis, des durées et des coûts d'hospitalisation. Ces codes pour la France ont été définis par le ministère de la santé et sont connus sous le terme de « PMSI ».

30 Actuellement toute structure d'hospitalisation retrace manuscritement, sous forme d'un codage PMSI, l'historique du patient dans la structure hospitalière.

Une telle façon d'opérer particulièrement fastidieuse en soi occupe bien souvent plusieurs personnes sous la responsabilité du médecin en charge de l'application du PMSI.

La vulgarisation des matériels et logiciels informatiques permet un traitement
35 informatique particulièrement aisé des dossiers médicaux du patient. Cependant cette facilité de traitement offre en corollaire à des personnes non autorisées l'accès à des données strictement confidentielles. Outre la violation du secret, les données des dossiers médicaux se trouvent exposées à des effacements accidentels ou volontaires ou à des modifications accidentelles ou frauduleuses.

Le traitement informatique des données médicales ne trouve son intérêt que si d'une part il concerne l'ensemble des données, résultat d'examen compris (radiographie, séquences échographiques, séquences sonores Doppler) et si les formats utilisés pour l'enregistrement de ces données sont standards et largement utilisés.

- 5 Bien qu'il soit possible actuellement d'enregistrer numériquement des images dynamiques, les formats d'enregistrement utilisés par exemple du type « DAICOM » sont trop spécifiques et réservés aux seuls centres médicaux équipés de machines et logiciels adaptés.

Le coût élevé de ces machines et logiciels, réserve leurs utilisations aux seuls centres importants.

- 10 La numérisation d'images fixes par exemple des radiographies, bien que techniquement plus simple ne semble pas avoir été abordée de sorte que ces images sont encore fournies sur papiers argentiques avec tous les problèmes liés à l'utilisation de tels supports tels que nécessité d'utiliser des bains corrosifs pour le développement des images, bains qui doivent subir des traitements appropriés avant rejet. Un autre inconvénient lié à l'utilisation de tels supports est leur
- 15 coût relativement élevé. En moyenne, le coût du support et du développement se situe aux alentours d'une centaine de francs.

- Le développement de réseau du genre Internet ou Intranet, permet comme on le sait un échange rapide de données entre deux points géographiques distants l'un de l'autre, et la consultation à distance de données enregistrées. Il devient alors intéressant d'utiliser de tels
- 20 réseaux pour consulter et/ou modifier à distance les dossiers médicaux de patients clients d'un centre de soins médicaux, dont certains des services sont répartis sur une aire géographique relativement étendue, de la taille d'une ville.

- Un autre cas typique pour lequel il est utile d'utiliser de tels réseaux dans les buts précités est celui d'un médecin attaché à plusieurs centres de soins, possédant des disciplines
- 25 médicales différentes et qui suit tour à tour un même patient dans un centre et dans un autre.

Enfin, un autre cas est celui d'un médecin attaché à un centre de soins et qui se rend au chevet d'un patient client de ce même centre de soins.

- Bien que particulièrement avantageuse et peu coûteuse, l'utilisation de tels réseaux se heurte à leur manque de fiabilité en termes de confidentialités de données échangées. Il est bien sûr
- 30 connu de crypter les données, mais il est impératif que ces données ne puissent être lues que par le médecin en charge du patient ou par toute autre personne légalement autorisée à prendre connaissance de ces données.

- La présente invention a pour objet de résoudre les différents problèmes évoqués en proposant un système de traitement de données et de stockage qui ne réserve l'accès de
- 35 données confidentielles qu'à des personnes dûment habilitées.

Un autre but de la présente invention est un système de traitement des données qui rende techniquement difficile voire impossible au moins à des personnes non habilitées, la modification de données préalablement saisies et validées.

Un autre but de la présente invention est un système de traitement des données qui permette l'enregistrement de certaines données sur des CD ROM suivant des formats connus tels que JPEG ou MPEG.

5 Un autre but de la présente invention est un système de traitement de données qui rend techniquement difficile voire impossible, au moins à des personnes non habilitées, la modification de données préalablement enregistrées.

A cet effet, le système de traitement de données numériques par exemple des données médicales des dossiers médicaux de plusieurs patients, clients d'un ou plusieurs centres de soins, se caractérise essentiellement en ce qu'il comprend :

- 10 - au moins un premier ensemble de traitement des données comprenant au moins un serveur auquel sont connectés au moins une première base de données, au moins un module de saisie et d'enregistrement des dites données confidentielles dans ladite première base de données, lesdites données avant enregistrement étant cryptées à l'aide d'une première clé publique enregistrée dans une mémoire du serveur, ladite mémoire contenant aussi une première clé
- 15 privée corrélée à la première clé publique, ledit premier ensemble comportant en outre au moins un module de lecture des données enregistrées pourvu d'un lecteur d'un support avec mémoire contenant au moins une clé utilisateur, corrélée au couple première clé publique et première clé privée, cette clé utilisateur étant utilisable pour le décryptage de toutes les données cryptées ou d'une partie de ces dernières seulement, selon le niveau d'autorisation attaché à ladite clé
- 20 utilisateur,
- un second ensemble de traitement et de stockage des données, comprenant au moins premier serveur auquel sont connectés au moins une première base de données dans laquelle sont archivées les données confidentielles préalablement enregistrées dans la première base de données du premier ensemble de traitement, ledit second ensemble de traitement étant
- 25 indépendant du premier et étant connectable à ce dernier par des lignes téléphoniques et/ou par des lignes spécialisées, ledit second ensemble étant de plus pourvu d'un serveur constituant domaine racine, ledit serveur générant un certificat d'authentification racine comprenant une clé racine publique et une clé racine privée, et ledit domaine racine étant apte pour chaque premier ensemble à générer au moins un certificat d'authentification secondaire composé de ladite
- 30 première clé publique et de ladite première clé privée et pouvant recevoir notamment du premier ensemble de traitement des demandes de transfert de copie des données archivées, ledit second ensemble en réponse à cette demande, assurant le cryptage des dites données avec la première clé publique avant de transférer les dites données vers le premier ensemble de données

35 Une telle architecture confère au système de traitement un haut niveau de sécurité, l'accès aux données étant réservé aux seules personnes habilitées et lesdites données étant systématiquement cryptées avec la clé publique du destinataire avant leur transfert du second ensemble de traitement vers le premier ensemble de traitement. En outre l'archivage numérique de toutes les données permet maintenant un traitement statistique de ces dernières.

De plus la saisie de toutes les données par le biais de moyens informatiques, tant logiciels que matériels autorise une automatisation poussée de l'élaboration et de la tenue des formulaires du PMSI.

5 Selon une autre caractéristique de l'invention, les données alphanumériques, saisies au niveau du premier ensemble, sont après validation de la saisie et avant cryptage, codées selon le format HTML.

Ce langage à balises, utilisé comme on le sait pour coder des pages WEB présente deux avantages majeurs, il rend très difficile la modification des données d'une part et se prête particulièrement bien à des transferts par le biais du réseau Internet.

10 Selon une autre caractéristique de l'invention, le premier ensemble comprend plusieurs bases de données dont une au moins reçoit les fichiers numériques d'images fixes comme des radiographies.

15 Selon une autre caractéristique de l'invention, le premier ensemble de traitement comprend plusieurs bases de données dont une au moins reçoit les fichiers numériques d'images dynamiques telles qu'échographie.

Selon une autre caractéristique de l'invention, le premier ensemble est équipé de plusieurs bases de données dont une au moins reçoit les fichiers numériques de séquences sonores par exemple Doppler.

20 Ainsi les données en fonction de leurs natures sont stockées sur des supports différents ce qui diminue le temps d'accès aux dites données.

25 Selon une autre caractéristique de l'invention, l'un au moins module de consultation du premier ensemble de données est constitué par un terminal du type micro-ordinateur connecté aux bases de données et possédant un lecteur de carte utilisateur, ledit micro-ordinateur étant équipé d'une carte vidéo prévue avec deux sorties connectées à deux écrans vidéo pour l'affichage simultané sur l'un, des images fixes ou dynamiques et sur l'autre des éventuels commentaires écrits associés à aux dites images fixes ou dynamiques.

On comprend tout l'intérêt d'une telle architecture puisqu'elle permet l'affichage simultané sur un écran d'une image par exemple une image radiologique et sur l'autre écran du diagnostic établi par le médecin en charge de l'examen.

30 Selon une autre caractéristique de l'invention, le second ensemble de traitement est équipé d'un serveur réseau Internet.

Par ce biais, un médecin attaché à un centre de soin, sans être présent dans ledit centre pourra consulter à distance le dossier médical de l'un de ses patients.

35 Selon une autre caractéristique de l'invention, le second ensemble de traitement est équipé d'un serveur de courrier électronique associé à une base de données dans laquelle sont introduites les adresses Internet des personnes autorisées à envoyer et recevoir les données confidentielles et une autre base de données contenant les premières clés publiques de chacune de ces personnes.

40 Selon encore une autre caractéristique de l'invention, le serveur Internet du second ensemble de traitement pilote un site Internet comportant une partie publique accessible à toutes

personnes intéressée, regroupant diverses données publiques non confidentielles relatives au premier ensemble de traitement et une partie privée accessible aux titulaires d'une clé d'utilisation.

5 Selon une autre caractéristique de l'invention, le serveur de réseau Internet intègre un moteur spécialisé de recherche des possesseurs des adresses Internet et des patients clients.

Selon une autre caractéristique de l'invention, le premier ensemble de traitement est doté d'une adresse Internet et l'accès via le réseau Internet au premier ensemble de traitement et aux données confidentielles que ce dernier possède tant au niveau de ses propres bases de données que des bases de données du second ensemble de traitement est validé par le serveur
10 de clé du second ensemble de traitement.

Le système de traitement de données confidentielles telles que les données médicales de dossiers médicaux de patients clients d'un ou plusieurs centres de soins comprend au moins un premier ensemble de traitement des données, logé physiquement dans le premier centre de soin et un second ensemble de traitement et de stockage des données situé à distance du
15 précédent et connecté à ce dernier par des liaisons filaires directes et/ou par des liaisons téléphoniques du genre RTC (Réseau téléphonique commuté) ou RNIS (Réseau numérique à intégration de service) ou bien par des lignes spécialisées aptes au transfert des données numériques sous fort débit et assurant une liaison filaire directe entre les deux ensembles.

Le centre de soin peut être un centre hospitalier ou bien un service de ce dernier.

20 Le centre de soin sera équipé d'un serveur de réseau connu en soi auquel sera ou seront connecté(s) un ou plusieurs sous-réseaux protégés, le tout étant architecturé selon la technique du tunnel. Pour mémoire cette technique consiste, dans un réseau global en la définition de certaines classes d'adresses qui vont correspondre respectivement aux divers sous-réseaux, chaque sous-réseau n'étant accessible que par un seul accès.

25 On limite aussi grandement les risques de piratage, l'accès n'étant ouvert que pendant la durée d'un transfert de données entre le sous-réseau et le serveur de réseau global.

Chaque sous-réseau sera constitué d'un ou plusieurs micro-ordinateurs du genre PC connectés les uns aux autres selon une technique connue. Typiquement chaque micro-ordinateur possède une unité centrale à laquelle sont connectés un clavier, un dispositif de
30 pointage et au moins un dispositif d'affichage tel qu'un écran vidéo, ou autre.

Il va de soi que chaque sous-réseau ou même le réseau dans sa globalité peut n'être constitué que d'un seul micro-ordinateur.

De même dans la mesure où est utilisé en tête de chaque réseau ou de chaque sous-réseau un serveur de réseau, les micro-ordinateurs pourront être remplacés par des postes
35 terminaux.

Les micro-ordinateurs et/ou les postes terminaux constitueront des modules de saisie et/ou de consultation.

Les différents sous-réseaux pourront équiper les différents services d'un même centre hospitalier. Ces différents sous-réseaux seront équipés d'une ou plusieurs bases de données qui
40 leur seront propres et qui pourront être inaccessibles aux autres sous réseaux et seront

connectés cependant à une base de données commune qui pourra contenir des données générales en rapport avec l'identité de chaque patient, de ses antécédents médicaux et de son historique médical.

Ces données seront saisies à l'aide des modules de saisie et après validation de la
5 saisie seront enregistrées dans la base de données. Pour éviter toutes modifications ultérieures, accidentelles ou frauduleuses, ces données, avant enregistrement, pourront être converties au selon le langage à balises HTML (Hyper Text Markup Language).

Comme on le sait ce langage, largement connu est utilisé pour le codage des pages « WEB ». Pour renforcer encore la sécurité des données, l'accès aux pages WEB relatives à ces données
10 sera sécurisé par codage selon le format SSL.

Les bases de données propres à chaque sous-réseau pourront contenir le résultat d'examens effectués dans le service médical correspondant. Selon la spécialité médicale du service, pourra être prévue une base de données relative aux commentaires écrit établis par le médecin chargé de l'examen médical.

15 Le résultat d'un examen peut aussi être matérialisé par des images fixes par exemple de radiographie, des images animées ou des sons. La plupart des machines utilisées pour mener à bien l'examen possèdent soit des sorties sur lesquelles est présent soit un signal vidéo fréquence, représentatif de l'image obtenue, soit un signal audio fréquence représentatif par exemple d'une séquence sonore Doppler.

20 À ces différentes machines sont associés des moyens convertisseurs analogiques numériques connectés aux sorties analogiques vidéo fréquences ou audio fréquence de ces machines afin de numériser le signal produit.

Le signal numérique en résultant sera traité à l'aide d'un micro-ordinateur et d'un logiciel spécifique, connu en soit afin de réaliser un fichier numérique, de l'image fixe ou animée ou du
25 son.

Ainsi chaque sous-réseau pourra être équipé d'une base de données contenant les fichiers numériques des images fixes, une base de données contenant les fichiers numériques des images animées et une base de données contenant les fichiers sons. Ces différents fichiers pour un même examen constituent les différentes composantes de ces derniers. Ces différentes
30 composantes étant réparties physiquement sur plusieurs unités de stockages, elles seront indexées de façon que par appel de l'une d'entre elles en vu de la consultation, les autres composantes soient recherchées et puissent être affichées ainsi que le dossier du patient et l'historique médical.

Préférentiellement, les fichiers numériques relatifs aux images fixes seront compressés
35 selon le format JPEG, tandis que les images animées seront converties au format MPEG. Les sons seront convertis au format MP3 ou autre.

Ces formats sont largement répandus et sont reconnus par la plupart des matériels et logiciels informatiques. L'intérêt d'une telle conversion est grand. En effet il n'est plus besoin de produire des images sur papier argentique coûteux en soi puisque par l'utilisation de ces formats elles
40 peuvent maintenant être enregistrées sur des supports du genre CD ROM qui seront remis au

patient. Pour cette raison à chaque sous-réseau pourra être associée une station de gravage de CD ROM constituée par un micro-ordinateur équipé d'un graveur de CD ROM et de logiciels adaptés, ce micro-ordinateur étant connecté au réseau ou sous-réseau.

Les différents fichiers de données avant leur enregistrement dans les bases de données
5 correspondantes sont cryptés à l'aide d'une clé publique à laquelle est associée une clé privée de décryptage.

À partir de ce couple de clé, inscrit dans une mémoire du serveur de réseau ou de sous-réseau, seront générées des clés utilisateurs qui seront distribuées aux différents utilisateurs du sous-réseau. À chacune de ces clés sera attaché un niveau d'autorisation quant à la nature des
10 données consultables par le détenteur de la clé. Ainsi le personnel administratif attaché au service médical ne pourra pas accéder aux résultats des examens, mais il pourra avoir accès aux données purement administratives concernant le patient. En revanche, le personnel de santé, infirmières et médecins, pourra avoir accès à l'ensemble du dossier médical du patient.

Selon la forme préférée de réalisation, les clés utilisateurs seront inscrites chacune sur
15 un support du type carte à puce, plus précisément ces clés seront inscrites dans une zone mémoire de la carte. Les différents micro-ordinateurs ou terminaux du réseau seront équipés de lecteur de carte à puce pour lire la ou les clés contenues dans les mémoires de ces dernières et déterminer le niveau d'autorisation de son titulaire. Il va de soi que le micro-ordinateur ou le serveur sera équipé de logiciels connus en soi, adaptés à la lecture de la carte et à
20 l'interprétation des données qu'elle renferme.

Préférentiellement à la clé est attaché un code individuel personnalisé connu sous le nom de code « PIN », dont la saisie manuelle active les fonctions de la carte à puce. Sans la saisie préalable de ce code, le micro-ordinateur ne pourra pas lire la ou les clés de la carte et n'affichera aucune donnée.

L'un des postes de consultation pourra être équipé de deux écrans et d'une carte vidéo à deux sorties. L'une des sorties sera connectée au premier écran, l'autre sortie au second. De plus ce poste de consultation pourra être équipé d'une carte son et d'enceintes acoustiques connectées à cette carte son. Ainsi sur ce poste de consultation, le médecin autorisé pourra
25 consulter tant les images et/ou les sons que les commentaires associés. Il va de soi que ce poste de consultation sera équipé d'un lecteur de carte à puce pour les mêmes raisons que
30 précédemment énoncées.

Les divers fichiers numériques inscrits dans les diverses bases de données ou bien au terme d'une période de temps prédéterminée sont transférés vers des bases de données que possède le deuxième ensemble de traitement, ce dernier constituant alors un site miroir.

Préférentiellement le contenu des bases de données est transféré sur des bandes magnétiques d'un type connu ou autre support d'enregistrement. Ces supports pourront être adressés par voie postale au second ensemble de traitement ou leurs contenus pourront être transférés par le biais des lignes téléphoniques ou spécialisées au deuxième ensemble de
35 traitement.

Les bases de données constituées à l'aide de ces bandes magnétiques pourront être consultées à distance depuis le premier ensemble de traitement de données. À cet effet, comme dit précédemment, le premier ensemble de traitement de données est connecté soit par ligne téléphonique soit par liaison filaire directe au deuxième ensemble de traitement et plus

5 précisément à un serveur que possède ce dernier. Physiquement ces banques de données seront constituées par les supports d'enregistrement, en l'espèce ces bandes magnétiques et par des moyens de lecture de support d'enregistrement en l'occurrence des lecteurs de bandes magnétiques. Il existe différentes sortes de bandes magnétiques, mais de préférence seront utilisées des bandes de très grande capacité. Les bandes magnétiques seront stockées dans

10 des unités de stockage du type magasin et seront manipulées entre le magasin et le dispositif de lecture et inversement par un bras manipulateur mobile dont le déplacement est contrôlé et commandé par le serveur correspondant du deuxième ensemble de traitement de données. Ce serveur sera capable de piloter et contrôler le lecteur de support d'enregistrement et avec un logiciel approprié, de lire les données inscrites sur le support introduit dans le lecteur et plus

15 précisément d'abord le répertoire relatif aux différents enregistrements que contient le support.

Préférentiellement, pour chaque premier ensemble sera prévue une ou plusieurs unités de stockage, cette unité de stockage ne contenant que les supports d'enregistrement propre à ce premier ensemble de traitement.

Il y a lieu de noter que plusieurs premiers ensembles de traitement pourront être

20 connectés à un unique deuxième ensemble de traitement et que chaque premier ensemble de traitement possèdera sa propre liaison avec le deuxième ensemble de traitement, soit sa propre ligne filaire dans le cas d'une liaison directe, soit son propre numéro téléphonique d'appel dans le cas d'une liaison par le réseau téléphonique.

L'intérêt d'une telle disposition est l'identification de l'appelant en l'espèce l'identification

25 du premier ensemble de traitement.

Le deuxième ensemble de traitement comprend aussi un serveur constituant domaine racine apte à générer un certificat d'authentification racine comprenant une clé racine publique et une clé racine privée. Le domaine racine pour chaque premier ensemble de traitement génère au moins un certificat d'authentification secondaire composé de la clé publique et de la clé privée

30 attachées audit premier ensemble.

Le serveur du deuxième ensemble de traitement en réponse à une demande de transfert de données numériques est donc apte à identifier le premier ensemble mais aussi le degré d'autorisation de la personne qui en fait la demande par lecture à distance de la carte à puce. Si la personne qui formule la demande n'a pas introduit sa carte à puce dans le lecteur de son

35 micro-ordinateur ou ne possède pas les autorisations requises, sa demande ne sera pas traitée.

Physiquement séparé des autres bases de données, le second ensemble de données comprend une autre base de données contenant les clés publiques des différents premiers ensembles de traitement de données, de sorte qu'avant transfert, les données confidentielles demandées sont cryptées par le serveur avec la clé publique du destinataire.

Dans la pratique le demandeur de l'information, quand il se connecte au premier ensemble de données ouvre une session terminal et reçoit du serveur du deuxième ensemble de données des messages lui demandant d'introduire sa carte à puce. S'il possède les autorisations requises le serveur du deuxième ensemble de données lui transférera un répertoire relatif au contenu de sa base de données. Il aura alors la faculté de choisir les documents qu'il souhaite transférer.

Avantageusement le deuxième ensemble de traitement comprend un serveur Internet de façon que des personnes autorisées puissent consulter à distance et/ou télécharger le dossier médical de leurs patients. De plus chaque premier ensemble de traitement possède son adresse Internet, mais le serveur Internet correspondant est celui du deuxième ensemble de traitement de données. Ainsi en se connectant à l'adresse Internet du premier ensemble de traitement de données, la personne autorisée se connecte en fait sur le deuxième ensemble de traitement de données. De la même façon que précédemment, le serveur avant de traiter la demande vérifiera à distance d'une part la présence de la carte à puce dans le lecteur et d'autre part le degré d'autorisation que possède cette carte avant de traiter la demande.

Le deuxième ensemble de traitement de données possèdera également un serveur de courrier électronique associé à une base de données contenant les adresses électroniques des premiers ensemble de traitement et/ou des personnes autorisées à émettre ou à recevoir du courrier électronique.

Les courriers reçus dans la boîte à lettre électronique du destinataire seront cryptés par le serveur du deuxième ensemble de traitement avec la clé publique de ce destinataire.

Préférentiellement, le serveur de réseau Internet intègre un moteur spécialisé de recherche des possesseurs des adresses Internet et des patients clients du ou des premiers ensembles de traitement. L'accès à ce moteur de recherche sera réservé aux seuls détenteurs d'une clé utilisateur. Par ailleurs pour ce qui concerne les patients et leurs dossiers médicaux, ils ne pourront effectuer leur recherche que parmi ceux clients du centre médical auquel ils appartiennent.

Enfin, le serveur Internet du second ensemble de traitements pilote pour chaque premier ensemble un site public accessible à toutes personnes intéressées et regroupant diverses données publiques relatives au premier ensemble de traitement et un site privé accessible aux seuls possesseurs d'une clé d'utilisation. Par l'intermédiaire de cette partie privée, le possesseur d'une clé d'utilisation pourra accéder, en fonction du degré d'autorisation à tout ou partie des données confidentielles ainsi qu'au moteur de recherche spécialisé.

Il va de soi que la présente invention s'applique au traitement de toutes données et dossiers confidentiels et n'est pas limitée au seul domaine médical. Il est bien évident qu'elle peut recevoir toutes variantes sans pour autant sortir du cadre du présent brevet.

REVENDECATIONS.

1/ Système de traitement de données confidentielles telles que les données médicales des dossiers médicaux de plusieurs patients, clients d'un ou plusieurs centres de soins, caractérisé en ce qu'il comprend :

- 5 - au moins un premier ensemble de traitement des données comprenant au moins un serveur auquel sont connectés au moins une première base de données, au moins un module de saisie et d'enregistrement des dites données confidentielles dans ladite première base de données, lesdites données avant enregistrement étant cryptées à l'aide d'une première clé publique enregistrée dans une mémoire du serveur, ladite mémoire contenant aussi une première clé
- 10 privée corrélée à la première clé publique, ledit premier ensemble comportant en outre au moins un module de lecture des données enregistrées pourvu d'un lecteur d'un support avec mémoire contenant au moins une clé utilisateur, corrélée au couple première clé publique et première clé privée, cette clé utilisateur étant utilisable pour le décryptage de toutes les données cryptées ou d'une partie de ces dernières seulement, selon le niveau d'autorisation attaché à ladite clé
- 15 utilisateur,
- un second ensemble de traitement et de stockage des données, comprenant au moins premier serveur auquel sont connectés au moins une première base de données dans laquelle sont archivées les données confidentielles préalablement enregistrées dans la première base de données du premier ensemble de traitement, ledit second ensemble de traitement étant
- 20 indépendant du premier et étant connectable à ce dernier par des lignes téléphoniques et/ou par des lignes spécialisées, ledit second ensemble étant de plus pourvu d'un serveur constituant domaine racine, ledit serveur générant un certificat d'authentification racine comprenant une clé racine publique et une clé racine privée, et ledit domaine racine étant apte pour chaque premier ensemble à générer au moins un certificat d'authentification secondaire composé de ladite
- 25 première clé publique et de ladite première clé privée et pouvant recevoir notamment du premier ensemble de traitement des demandes de transfert de copie des données archivées, ledit second ensemble en réponse à cette demande, assurant le cryptage des dites données avec la première clé publique avant de transférer les dites données vers le premier ensemble de données

- 30 2/ Système de traitement selon la revendication 1, caractérisé en ce que les données alphanumériques, saisies au niveau du premier ensemble, sont après validation de la saisie et avant cryptage, codées selon le format HTML.

3/ Système de traitement selon la revendication 1 ou la revendication 2, caractérisé en ce que le support sur lequel est inscrite la clé utilisateur est du type carte à puce.

- 35 4/ Système de traitement selon l'une quelconque des revendications précédentes, caractérisé en ce que le premier ensemble comprend plusieurs bases de données dont une au moins reçoit les données alphanumériques.

- 5/ Système de traitement selon l'une quelconque des revendications précédentes, caractérisé en ce que le premier ensemble comprend plusieurs bases de données dont une au
- 40 moins reçoit les fichiers numériques d'images fixes comme des radiographies.

6/ Système de traitement selon l'une quelconque des revendications précédentes, caractérisé en ce que le premier ensemble de traitement comprend plusieurs bases de données dont une au moins reçoit les fichiers numériques d'images dynamiques telles qu'échographie.

5 7/ Système de traitement selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est équipé de plusieurs bases de données dont une au moins reçoit les fichiers numériques de séquences sonores par exemple Doppler.

8/ Système de traitement selon la revendication 5, caractérisé en ce que les fichiers numériques relatifs aux images fixes sont au format JPEG.

10 9/ Système de traitement selon la revendication 6, caractérisé en ce que les fichiers relatifs aux images dynamiques sont au format MPEG.

10/ Système de traitement selon la revendication 7, caractérisé en ce que les fichiers numériques relatifs aux séquences sonores sont au format MP3.

15 11/ Système de traitement selon l'une quelconque des revendications précédentes, caractérisé en ce que l'un au moins module de consultation du premier ensemble de données est constitué par un terminal du type micro-ordinateur connecté aux bases de données et possédant un lecteur de carte utilisateur, ledit micro-ordinateur étant équipé d'une carte vidéo prévue avec deux sorties connectées à deux écrans vidéo pour l'affichage simultané sur l'un, des images fixes ou dynamiques et sur l'autre des éventuels commentaires écrits associés à aux dites images fixes ou dynamiques.

20 12/ Système de traitement selon l'une quelconque des revendications précédentes, caractérisé en ce que le second ensemble de traitement est équipé d'un serveur réseau Internet.

25 13/ Système de traitement selon la revendication 12, caractérisé en ce que le second ensemble de traitement est équipé d'un serveur de courrier électronique associé à une base de données dans laquelle sont introduites les adresses Internet des personnes autorisées à envoyer et recevoir les données confidentielles et une autre base de données contenant les premières clés publiques de chacune de ces personnes.

30 14/ Système de traitement selon la revendication 12 ou la revendication 13, caractérisé en ce que le serveur Internet du second ensemble de traitement pilote un site Internet comportant une partie publique accessible à quiconque regroupant diverses données publiques non confidentielles relatives au premier ensemble de traitement et une partie privée accessible aux titulaires d'une clé d'utilisation.

15/ Système de traitement selon l'une quelconque des revendications 12 à 14, caractérisé en ce que le serveur de réseau Internet intègre un moteur spécialisé de recherche des possesseurs des adresses Internet et des patients clients.

35 16/ Système de traitement selon l'une quelconque des revendications 12 à 15, caractérisé en ce que le premier ensemble de traitement est doté d'une adresse Internet et que l'accès via le réseau Internet au premier ensemble de traitement et aux données confidentielles que ce dernier possède tant au niveau de ses propres bases de données que des bases de données du second ensemble de traitement est validé par le serveur de clé du second ensemble
40 de traitement de données.